06.10.2004

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月１４日

出願番号
Application Number: 特願２００３－３５３６９１

[ST. 10/C]: [ＪＰ２００３－３５３６９１]

出願人
Applicant(s): 松下電器産業株式会社





２００４年１１月１２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１０２３３

【書類名】　特許願
【整理番号】　2048150017
【特記事項】　特許法第３６条の２第１項の規定による特許出願
【提出日】　平成15年10月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/00
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　シェン　メイ・シェン
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　ジ・ミン
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　ファング・ゾンヤン
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　妹尾　孝憲
【特許出願人】
　【識別番号】　000005821
　【住所又は居所】　大阪府門真市大字門真１００６番地
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100086405
　【弁理士】
　【氏名又は名称】　河宮　治
　【電話番号】　06-6949-1261
　【ファクシミリ番号】　06-6949-0361
【選任した代理人】
　【識別番号】　100098280
　【弁理士】
　【氏名又は名称】　石野　正弘
　【電話番号】　06-6949-1261
　【ファクシミリ番号】　06-6949-0361
【手数料の表示】
　【予納台帳番号】　163028
　【納付金額】　35,000円
【提出物件の目録】
　【物件名】　外国語特許請求の範囲　1
　【物件名】　外国語明細書　1
　【物件名】　外国語図面　1

【物件名】　外国語要約書　1
【包括委任状番号】　9602660

【書類名】外国語特許請求の範囲

2 **WHAT IS CLAIMED IS:**

(1) Content Server with Digital Content Protection and Digital Rights Expressions, comprising the following steps of:

Packaging a digital content by creating a set of digital descriptions including its content identifier (Content ID), or sub content ID, rights and protections descriptions and other kinds of metadata;

Creating a wrapper or container to hold all the above said metadata, and the container is called DID (Digital Item Declaration) in MPEG-21 scope;

Creating a holder which is to hold rights and protection descriptions, and here the holder is called IPMP Control Graph or REL-IPMP Control Graph;

Placing a flag in the first place in the said holder to indicate if the said content is protected or free copy;

Attaching a flag 1 to the said content to indicate if there is watermarking applied to the said content;

Attaching a flag 2 to the said content to indicate if the said content is protected;

Attaching a flag 3 to the said content to indicate if the said content is digital signed;

Attaching a flag to the said rights metadata or other groups of metadata, respectively, to indicate if the said rights metadata or other kinds of metadata is digital signed;

Encrypting and protecting the said content with the said content ID using a selected or defined encryption tool with its pre-defined or registered ToolID;

Embedding watermarks to the said content with the said content ID using a selected or defined watermarking tool with its pre-defined or registered ToolID;

Digital signing the said rights or other kinds of metadata using a selected or defined signing tool with its pre-defined or registered ToolID;

Creating descriptions which are used to describe the above said encryption, watermarking, and digital signing with the further information;

Arranging the said above flags and descriptions regarding rights and protection applied to the said content in the defined format, which could be in XML or binary;

Placing the said arranged data in the said holder of IPMP Control Graph or REL-IPMP Control Graph, and

Carrying the said such holder as rights and protection information in DID container in MPEG-21 scope, or other places in other application domain.

(2) Content Server with Digital Content Protection and Digital Rights Expressions, whereas Encrypting and protecting the said content with the said content ID using a selected or defined encryption tool with its pre-defined or registered ToolID in claim 1, further comprising the following steps of:

Digital signing the said content with the said content ID using a selected or defined signing tool with its pre-defined or registered ToolID.

(3) Content Server with Digital Content Protection and Digital Rights Expressions, whereas Creating descriptions which are used to describe the above said encryption, watermarking, digital signing with the further information in claim 1, further comprising the following steps of:

Placing the key information used for the said encryption in KeyData holder in IPMP Control Graph or REL-IPMP Control Graph directly, or a pointer to point to a location;

Encrypting the encryption key again to generate key license;

Carrying the said key license in rights data, or IPMP Control Graph/REL-IPMP Control Graph, or in DID in MPEG-21 scope, and

Placing watermark descriptions including interfaces or API which is used in the said holder of IPMP Control Graph/REL-IPMP Control Graph.

(4) Content Server with Digital Content Protection and Digital Rights Expressions, whereas Carrying the said such holder as rights and protection information in DID container in MPEG-21 scope, or other places in other application domain in claim 1, further comprising the following steps of:

Carrying the static part of the descriptions in the same channel or different channels or out of the band when the said content is delivered via network, for example carrying over SDP (Section Description Protocol) for RTP streaming or content distribution over RTP, and

Carrying time-variant part of the data in segments or packets to synchronize with video or audio data which is to protect, for example carrying time-variant key information in RTP header or as special packets as for video and audio data.

(5) Content Server with Digital Content Protection and Digital Rights Expressions whereas in claim 1 encryption could be done using a defined tool as default with a defined ToolID in certain application domain, digital signing could be done using a defined tool as default with a defined ToolID in certain application domain, and other protection such as watermarking could be done by defining an interface or API to achieve flexibility.

(6) Content Server with Digital Content Protection and Digital Rights Expressions whereas in claim 1 the said REL-IPMP Control Graph means to extend the existing REL of MPEG-21 or other rights expression language to contain protection description information, where IPMPX is defined as the flag used to represent the extension part of protection from the existing REL.

【書類名】外国語明細書

# 1 TITLE OF THE INVENTION

Content Server with Digital Content Protection and Digital Rights Expressions

# 3 DETAILED DESCRIPTION OF THE INVENTION

## 3.1 Industrial Field of Utilization

The present invention relates to Digital Rights Management (DRM) or Intellectual Property Management and Protection (IPMP) for a generic digital content, especially relates to the protection and management of a digital content independent of any data format.

## 3.2 Background and Prior Art

As various kinds of network are widely deployed, it will be demanded that digital content can be delivered and distributed to user via such network besides using CD, DVD. The corresponding issue is raised by content owner. Is it secure to sell their content in this way?

As hard disk or other storage embedded device become more and more, another issue is that how the content protection technique can ensure the entitled rights to be exercised correctly.

As many different digital formats exist to use for packaging content in digital form for easy transmitting over various network, question arises as how the protection technology can be cross-used among different digital formats.

At the same time users have more demands on the convenience with low cost for enjoying content, even sharing with their friends if they purchase such rights, to have rich user experience.

Conflict is always there since content owner cares for any illegal copy so that content providers are trying to protect content in their own proprietary ways due to lacking of the open protection techniques in the market at that time.

This not only brings a big barrier for content owner to sell content, but also brings a heavy cost for CE (consumer electronics) manufacturers to produce different versions of the product just for matching with various protection techniques which content provider use.

MPEG-21 is trying to define a generic framework to enable transparent and augmented use of digital content across a wide range of networks and devices used by different communities. How to protect the contents when they are being used across network or devices, becomes a very important item in MPEG-21, which is the part 4 of MPEG-21, called MPEG-21 IPMP (Intellectual Property Management and Protection)

In the past, people working on MPEG-4/2 IPMP Extension were required to define a content protection scheme based on MPEG-4/2 system since the aim is to protect any content if they are packaged in MPEG-4/2 format.

In MPEG-21, a Digital Item (DI) is defined as a structured digital object for any digital content with a standard representation, identification and description, and it will be used as the fundamental unit of interchange, distribution and transaction within MPEG-21 framework.

The Digital Item is declared and expressed using XML by Digital Item Declaration (DID). Besides a digital content which is represented as media resources in MPEG-21, such as video, music, image, the DID provides the flexible structure to include various kinds of functional metadata. Such metadata is supposed to describe media resource format, to specify resource protection scheme, to give the resource an identification name, to provide User preference, etc.

Besides the core part of DID technology, some other key technologies have also been elaborately developed or are under development. Digital Item Identification (DII), Digital Item Adaptation (DIA), Intellectual Property Management and Protection (IPMP), REL (Rights Expression Language)/RDD (Rights Data Dictionary), as well as ER (Event Reporting) are all the important technologies for extensively exploiting the Digital Items' usage. All the functional metadata defined by these technologies can be placed into a DID document to aid the actual media resource consumption.

A content protection and management mechanism is highly requested to address most of the requirements raised by many different application domains, especially in the scope of MPEG-21 domain, to reflect the market needs.

### 3.3 Problem to be Solved

The requirements on MPEG-21 IPMP are the problems to be targeted and solved here.

IPMP, especially MPEG-21 IPMP shall support the management and protection of intellectual property in descriptors and description schemes.

IPMP, especially MPEG-21 IPMP shall provide for interoperability so that content is able to be played anywhere.

IPMP, especially MPEG-21 IPMP should enable devices to dynamically discover, request, and obtain upgrades for supporting new media formats, IPMP tools and support.

IPMP, especially MPEG-21 IPMP shall provide mechanisms to reference Digital Item Descriptions as part of the language, make reference to external content descriptions.

IPMP, especially MPEG-21 IPMP shall provide mechanisms to associate Expressions with composite Digital Items.

IPMP, especially MPEG-21 IPMP shall provide mechanisms to reference Containers or other aggregations of Digital Items.

IPMP, especially MPEG-21 IPMP should flag that a particular Expression should be subject to protection. The protection itself (if any) is provided by an IPMP system controlling the Expression as a Digital Item.

IPMP, especially MPEG-21 IPMP shall provide mechanisms to reference authentication schemes.

IPMP, especially MPEG-21 IPMP shall provide mechanisms to ensure that the IPMP is independent of the format or delivery channel of Digital Items.

IPMP, especially MPEG-21 IPMP shall unambiguously articulate requirements relating to IPMP Tool and Features.

IPMP, especially MPEG-21 IPMP shall need to identify IPMP Tools and Features to build trusted IPMP implementations.

IPMP Tools and Features are components parts to build an IPMP-enabled Terminal or Peer. It should also possible for a Terminal or Peer to disclose its IPMP capability (IPMP Tools and Features). This makes it possible for a communicating Terminal or Peer to examine IPMP capability of another Terminal or Peer before deciding to engage with it.

### 3.4 Means of Solving the Problems

On the content packaging side:

By introducing the concept of IPMP Control Graph to refer to all the rights and protection information which is directly associated with the content

By defining IPMP Control Graph or REL-IPMP Control Graph as protection metadata holder to contain rights and protection information which is used to package and protect the content;

By placing rights & condition in the IPMP Control Graph or REL-IPMP Control Graph;

By placing content encryption information in the IPMP Control Graph or REL-IPMP Control Graph;

By placing watermarking information in the IPMP Control Graph or REL-IPMP Control Graph;

By placing rights protection information in the IPMP Control Graph or REL-IPMP Control Graph;

By placing and indicating key information which is used to encrypt content in the IPMP Control Graph or REL-IPMP Control Graph;

By placing key/license information in the IPMP Control Graph or REL-IPMP Control Graph, or in Rights, DID, or somewhere indicated by keyLocation;

By indicating which IPMP Tool is used for encryption, digital signing, watermarking with ToolID in the IPMP Control Graph or REL-IPMP Control Graph;

By associating rights and protection with the protected digital content or its sub content using content ID or DII and sub content ID;

By placing IPMP Control Graph or REL-IPMP Control Graph in DID container or other appropriate place in other application domains;

On the terminal side:

By parsing DID to retrieve content ID or sub content ID, and IPMP Control Graph or REL-IPMP Control Graph;

By parsing IPMP Control Graph or REL-IPMP Control Graph to retrieve Rights and Protection related descriptions;

By invoking IPMP tools which are used to protect the content or rights, or other metadata;

By retrieving key information from KeyData Holder directly of indirectly;

By retrieving a key license from a protected License Manager;

By un-protecting the protected content using the above obtained information;

By checking Rights' integrity using the tool indicated by ToolID;

By parsing the rights and conditions which are embedded with the content;

By retrieving watermarking descriptions and preparing for further action;

### 3.5 Operation of the Invention

On the content production side as shown in Figure 3, IPMP Control Graph is generated as shown in Figure 7, to contain all the rights and protection information which is directly associated with the content identified by content Identifier (CID) or DII if MPEG-21 could be used.

The content could be watermarked using certain watermarking tool to achieve certain functions, such as finger printing, persistent association, or copyright protection by embedding CID or other information.

The content can be encrypted by an IPMP tool with ToolIDXXX, where xxx is the number which is registered with RA (Registration Authority), to indicate which encryption algorithm is used. A default tool such as AES is defined for simple hardware to implement. The resulted Key information could be carried in IPMP Control Graph directly or by pointing to a location where the whole Key information data could be found. The encryption key can be further encrypted and finally a license could be generated and directly carried in either IPMP Control Graph, in REL data or other Rights Expression Data, or in DID itself, or in somewhere which can be indicated by KeyLocation indicator to be carried in IPMP Control Graph/REL/DID;

However the segments of key information would also possibly be packaged together with the associated content segments when the protected content is transmitted via network for synchronization purpose.

Rights can be expressed by an independent and existing technology standard such as REL defined in MPEG-21 or other Rights Expression methods, and such rights could be protected by digital signature for its integrity;

On the content consumption side as shown in Figure 4, a packaged content with rights and protection information is subjected to IPMP Control Graph parsing, from there it can be known if the content is protected and furthermore to determine whether the content is encrypted, watermarked, or rights is protected as well;

The corresponding protection tools would be invoked and acted on the protected object, the tools can be those normative tools defined by MPEG-21 standard and hence installed in the device, or the tools can be proprietary and identified by tool IDs which can be downloaded from a remote location;

Tool is identified by a registered Tool ID, which is a flag to tell terminal or device to prepare the corresponding tool or locate the tool beforehand;

The key information is retrieved from KeyData Holder defined and carried in IPMP Control Graph directly or indirectly, and it would also possibly be obtained in segment with the corresponding content segment to be protected if the content is distributed through network.

The license information can be obtained from License Manager which could be a temper resistant entity to prevent any disclosure of how a license is retrieved by a license manager.

Rights and content is un-protected by using the above key, key data, and protection tool. Rights is further parsed by Rights Parser to obtain the rights and conditions in clear form, so that the rights and conditions processing can be conducted.

Therefore the un-protected content can be played back, rendered, modified, deleted, or adapted if there is such rights entitled for the user;

### 3.6 Embodiments

As shown in Figure 1 for the prior art [see reference 1 and 2], a digital content is packaged by DID with possible protection associated.

The DID has defined a useful model (unit 1.1 in Figure 1) formed by a set of abstract terms and concepts such as **Container, Item, Component, Anchor, Descriptor, Condition, Choice, Selection, Annotation, Assertion, Resource, Fragment, Statement**, etc (e.g. shown in Figure 1 unit 1.6, 1.7, 1.8) for defining Digital Items.

Module 1.2 shown in Figure 1 is the overall IPMP Control Information used for all the items to be protected inside this container. Module 1.3 and 1.4 are the specific protection information which is associated to the protected content. Module 1.5 is the DII to indicate the content ID.

The further improvements over the Prior Art are:

Since DID is to address static relation among each elements and it can be treated as file format, rights and protection information can be directly associated to its protected content as IPMP_Control_Graph, shown in Figure 3.

On the other hand, key information can be carried from KeyData Holder in IPMP_Control_Graph directly or indirectly. It could also be segmented when the content is delivered via network.

Rights which might be encrypted is carried separately or together with protection information.

Another Prior Art is shown in Figure 2 [see reference 3] for MPEG-21 IPMP Architecture.

The Rights Expression Language (REL) Engine in module 2.1 is the component that determines REL authorizations, given an authorization request and a set of licenses and root grants. The REL Engine uses the License Manager to help resolve authorization queries.

The Digital Item Manager in module 2.2 parses Digital Item Declarations within Digital Items. The Digital Item Manager also provides access to where the Digital Items are, and creates Digital Item iNstances in module 2.3. The Digital Item Manager passes to the License Manager any Licenses that are embedded within Digital Item Declarations.

The Digital Item iNstance in module 2.3 represents a Digital Item within a Trusted Domain. The Digital Item iNstance contains local metadata about the Digital Item, such as storage location and possibly information about content encryption keys.

The License Manager in module 2.4 supports the REL Engine by managing the persistent state of Licenses and their authorization or revocation status. The License Manager is also responsible for verifying the integrity of Licenses.

The Condition Processor in module 2.5 selects, evaluates and fulfills Conditions, and initiates the execution of authorized Operations (via the DIP Processor, generating a Right Exercise) once conditions are satisfied.

The IPMP User Session Manager in module 2.6 orchestrates the invocation of Digital Item Operations (via the Condition Evaluator), first making sure that proper authorization is obtained (via the REL Engine) and that conditions are evaluated (via the Condition Evaluator).

A Right Exercise in module 2.7 is a record of having exercised a right, *i.e.,* the invocation of a Digital Item Operation. It is maintained by the User Session Manager, and is used to associate the fulfillment of Conditions with the exercise of Rights.

The Digital Item Processing Engine in module 2.8 executes Digital Item Operations, including Digital Item Methods (DIMs), Digital Item Basic Operations (DIBOs) in module 2.9, and Digital Item eXtended Operations (DIXOs) in module 2.10. The DIMs are executed by a DIM Engine, the DIXOs by a DIXO Engine, and the DIBOs by a DIBO Library. The Digital Item Processing Engine updates the User Session State with process state information.

The big issue with Figure 2 is that there is no protection information to be processed, interpreted and transferred, especially when content is protected by several tools and rights is also protected using different tools. There is no clear picture for people to know how the content is protected and how it should be processed.

The second issue with Figure 2 is that the data flow from License Manager should not go to REL Engine since the existing REL engine defined in MPEG-21 REL only processes rights expression. The output from license manager could contain the encryption key which is used to decrypt the content controlled by an entity which should be IPMP Manager shown in Figure 9. The decryption itself can be done in IPMP Tools, DIP Processor, DIME, or DIBO, or DIXO.

The third issue with Figure 2 is that there is no data flow indication to indicate where those REL data comes from, for REL Engine to process. Such Rights Expression including rights conditions if they are expressed in MPEG-21 REL format, they could be carried as metadata together with DI in a DID container, and processed by DI Manager. DI Manager should be changed into DID Parser which only parses information by following what DID is defined.

The better rights and protection is designed based on the two cases. The first case is where the existing REL is employed for expressing the corresponding rights and conditions and a protection control mechanism is defined to take care of content protection including encryption, watermarking, key management. The second case is where the existing REL is extended by adding protection function which could include encryption, watermarking, key management, etc.

Both cases are elaborated in the following sections.

### 3.6.1 Content Packaging and Consumption with Separate Rights and Protection

As in Figure 3, it is shown on the content packaging side with rights and protection scheme. REL in module 3.8 is the existing rights expression language to be used to package the relevant rights with their conditions. Other parts through 3.3, 3.4, 3.5, 3.6, 3.7, 3.9, 3.11, and 3.13 are the protection related functions. The most important part is in module 3.15, which is the IPMP Control Graph. It can be carried in DID container in MPEG-21, but it also can be carried in other places in different application domains.

When the content is needed to transmit via network, normally it will be segmented, encrypted and stored as Resource somewhere, and the corresponding time-variant key is

stored as Key Information in KeyData Holder in IPMP Control Graph in module 3.9 directly or indirectly by pointing to a location.

For example when the protected content is transmitted over RTP, IPMP Control Graph can be carried in SDP (Section Description Protocol), while the key information can be carried in the RTP header or as special case for video and audio packet as long as there is synchronization among time-variant keys and the protected video or audio data.

Module 3.1 is to assign content ID, DII in MPEG-21 could be used here. If necessary sub content ID can be used and the protection can be associated with this sub content ID if the sub content need to be protected.

Module 3.2 is to place a flag in IPMP Control Graph to tell if the content is protected or free. Module 3.3 is to place a flag in IPMP Control Graph to indicate if there is watermarking embedded.

If there is watermarking embedded in the content, module 3.4 will assign watermarking (WM) ToolID for the WM tool used for this case, and ToolID is then recorded and placed in IPMP Control Graph. The module 3.5 will create WM Descriptions including watermarking Interface or API related information which is placed in IPMP Control Graph.

Module 3.6 is to determine if the content will be encrypted, and a flag for "Yes/No" will be placed in IPMP Control Graph in module 3.15.

Module 3.9 is to assign encryption ToolID for the encryption tool used for this case, and ToolID is then recorded and placed in IPMP Control Graph. The module 3.7 is to place Key information in KeyData Holder directly in IPMP Control Graph, or pointing by the Holder to other location.

The encryption key can be further encrypted in module 3.11, and 3.13, and the key as a license is eventually placed in IPMP Control Graph, REL, DID, or somewhere indicated by KeyLocation1.

Module 3.8 is to create and package rights with the corresponding conditions which conforms to the existing REL standard, and this part could be modified and edited by distribution agents in the content distribution value chain.

The module 3.10 is to protect the rights metadata by digitally signing the rights. Module 3.12 is to assign ToolID for the verification of the digital signature, and module 3.14 is to place the Entity_Key in IPMP Control Graph, or in DID, or in somewhere indicated by KeyLocation2.

The detail of module 3.15 is shown in Figure 7 (a) as an example in the case of MPEG-21 where XML based approach is used to express IPMP Control Graph. A DI (7.2, declared by a DID 7.1) consists of two Items (7.2, 7.3), each of which has their identification

scheme (7.4, 7.5) with respective attached media resource (7.8, 7.9). Module 7.6 shows the IPMP Control Graph mentioned above and Module 7.7 gives the actual rights expression (conditions and usage rules) linked to the resource.

Figure 4 shows the Terminal Processing Flow Chart to process protection & Packaging Information carried in IPMP Control Graph before a protected content could be consumed in module 4.18.

Module 4.1 is to parse DID and IPMP Control Graph information where DID parser is required only for the case IPMP Control Graph is carried in DID in MPEG-21 case.

In the case of content distribution over RTP network, IPMP Control Graph can be retrieved from SDP to obtain rights and protection description information except the key information if it is time-variant.

Module 4.2 is to detect if the content is protected or free. If it is free, it will be able to play back by module 4.18 for consumption. Otherwise there are three branches to go and check in module 4.3, 4.4, and 4.5, respectively.

Module 4.3 is to detect if the Rights is encrypted, module 4.4 is to detect if the content is encrypted, and module 4.5 is to detect if the content is watermarked.

If the rights is protected, module 4.6 is to invoke the protection tool with ToolID and module 4.7 is to check the integrity of the rights using the tool. If the integrity is successfully verified in module 4.8, the rights will be sent to module 4.9 for parsing the rights by REL Engine which conforms to the existing REL standard.

Module 4.11 is to process the rights and conditions attached to the content and store the entitled rights and conditions in a buffer. In module 4.19 those rights requested by the users are subjected to checking against the rights and conditions stored in the buffer.

If there is license carried in Rights, module 4.10 is to retrieve license from License Manager which may be temper resistant (TR) protected.

If the content is protected and encrypted, module 4.13 is to invoke the encryption tool indicated by ToolID carried in IPMP Control Graph, module 4.14 is to retrieve Key Information, and module 4.12 is to obtaining the key license from License Manager.

License Manager here could be protected by temper resistant technique if it is part of the terminal or somewhere in other places, since it will provide the actual license which the decryption engine will use to un-protect the content.

The encryption tool can be defined as default for most of the terminals to use in their implementation, while an IPMP ToolID is provided so that people can choose other than default encryption tool in their special domain. If the platform is allowed to download and use different encryption tool indicated by ToolID, it would achieve extensibility,

flexibility and renewability at the same time we will achieve interoperability across different domains.

Key Information could be retrieved from different places in the case of content delivery via various networks. This will depend on where you place key information. If you place them in RTP header, you can get them there, while if you place them as other packets like video and audio data, you can get them by following the same rules applied to video and audio. The time-variant key information is required to obtain in the same time when you need to decrypt the video and audio content.

Module 4.15 is to decrypt the content with the invoked tool, KeyData, and License, then passed to module 4.17 for further processing.

If the content is detected as watermarked in module 4.5, the watermarking tool with ToolID and its description data including interface will be invoked and prepared in module 4.16 for action which is up to user's request.

Finally module 4.17 is to exercise the rights which user is requested based on the entitled rights & conditions, and act on the un-protected content which is the output of module 4.15.

In Figure 4 Temper Resistant is used to protect the function of License Manager to provide license, Rights & Condition Processing to prepare the rights, even content decryption for obtaining un-protected content.

Figure 8 shows a modified IPMP Architecture with REL and IPMP Control Graph separately processed. Compared to the Rights and Protection (IPMP Related) functions in Figure 4 and Figure 8, it is clear that there are many IPMP related functions missing in the prior art of Figure 2. Only the blocks in blue color in Figure 4 which are the module 4.9 for REL Engine, module 4.10 and 4.12 for License Manager, and module 4.11 for Conditions Processing, are introduced in the prior art as shown in Figure 2. Such function blocks are module 2.1, module 2.4, and module 2.5 in Figure 2.

As shown in Figure 8, Module 8.11 is added for parsing and processing IPMP Control Graph information, and the corresponding results are passed to License Manager in module 8.4, REL related data passed to REL Engine in module 8.1 after its integrity is checked, and content protection and watermarking information passed to DI iNstanace in module 8.3 for further processing.

Decrypting, watermarking, etc. in module 8,12, could be conducted in module 8.8 if such method is defined in DIME, or in module 8.9 if it is defined as one function of DIBO, or in module 8.10 if it is an external function.

The line 8.14 is shown for the data flow from IPMP Control Graph processing module to REL Engine, and the line 8.15 is shown for the data flow from IPMP Control Graph processing module to NI iNstance.

The line 8.16 is shown for the data flow from License Manager to the un-protecting block in the module 8.12 for issuing a license.

Module 8.13 is for Event Reporting Engine which is placed in the same trusted domain compared to that in Figure 2.

TR means Temper Resistance module to be used to protect License Manager operation and Condition Processing Operation.

Other modules have the similar meaning as explained in Figure 2.

### 3.6.2 Content Packaging and Consumption with Mixed Rights and Protection

In this case, there is no clear boundary between rights and protection, and they are mixed. IPMP Control Graph can be considered as REL-IPMP Control Graph.

Based on the current MPEG-21 REL or other rights expression language, protection of content as well as indicating for how to protect the content is not defined. In this case the existing REL has to be extended to support such protection signaling.

As shown in Figure 5 which is based on Figure 3, Module 5.16 is considered as REL + Extension to support content protection signaling by extending the existing REL standard, and module 5.15 is changed into REL-IPMP Control Graph. Module 5.8 is the existing REL function.

Other modules have the same functions as explained above.

As in Figure 5, it is shown on the content packaging side with rights and protection scheme. REL in module 5.8 is the existing rights expression language to be used to package the relevant rights with their conditions. Other parts through 5.3, 5.4, 5.5, 5.6, 5.7, 5.9, 5.11, and 5.13 are the protection related functions. The most important part is in module 5.15, which is the REL-IPMP Control Graph. It is carried in DID container in MPEG-21, but it also can be carried in other places when it is used in different application domains.

When the content is needed to transmit via network, normally it will be segmented, encrypted and stored as Resource somewhere, and the corresponding time-variant key is stored as Key Information in KeyData Holder in REL-IPMP Control Graph in module 5.9 directly or indirectly by pointing to a location.

For example when the protected content is transmitted over RTP, REL-IPMP Control Graph can be carried in SDP (Section Description Protocol), while the key information can be carried in the RTP header or as special case for video and audio packet as long as they are synchronized among time-variant keys and the protected video or audio data.

Module 5.1 is to assign content ID, DII in MPEG-21 could be used here. Module 5.2 is to place a flag in REL-IPMP Control Graph to tell if the content is protected or free. Module 5.3 is to place a flag in REL-IPMP Control Graph to indicate if there is watermarking embedded.

If there is watermarking embedded in the content, module 5.4 will assign watermarking (WM) ToolID for the WM tool used for this case, and ToolID is then recorded and placed in REL-IPMP Control Graph. The module 5.5 will create WM Descriptions including watermarking Interface or API related information which is placed in REL-IPMP Control Graph.

Module 5.6 is to determine if the content will be encrypted, and a flag for "Yes/No" will be placed in REL-IPMP Control Graph in module 5.15.

Module 5.9 is to assign encryption ToolID for the encryption tool used for this case, and ToolID is then recorded and placed in REL-IPMP Control Graph. The module 5.7 is to place Key information in KeyData Holder directly in REL-IPMP Control Graph, or pointing by the Holder to other location.

The encryption key can be further encrypted in module 5.11, and 5.13, and the key as a license is eventually placed in REL-IPMP Control Graph, REL, DID, or somewhere indicated by KeyLocation1.

Module 5.8 is to create and package rights with the corresponding conditions which conforms to the existing REL standard, and this part could be modified and edited by distribution agents in the content distribution value chain.

The module 5.10 is to protect the rights metadata by digitally signing the rights. Module 5.12 is to assign ToolID for the verification of the digital signature, and module 5.14 is to place the Entity_Key in REL-IPMP Control Graph, or in DID, or in somewhere indicated by KeyLocation2.

The detail of module 5.15 is shown in Figure 7 (b) as an example in the case of MPEG-21 where XML based approach is used to express REL-IPMP Control Graph. The figure is similar to Figure 7 (a). It uses REL-IPMP Control Graph (7.10) to replace 7.6 and 7.7 modules as shown in Figure 7 (a) but act as similar function to represent all rights and protection information.

It can be seen from the Figure 7 (b) that the REL IPMP extension is defined here to contain not only rights expression but also protection descriptions, and such extension is done on the top of the existing MPEG-21 REL or other Rights expression language since they are originally defined just to express rights, conditions, as well as principles and issuers. The ipmpx shown in the XML expression in Figure 7 (b) is the part of the extension of REL for protection.

As shown in Figure 6 which is based on Figure 4, Module 6.19 is considered as REL + Extension to support content protection as well by the extended REL, and module 6.9 is the existing REL engine. Module 6.1 is changed into REL-IPMP Control Graph, and Module 6.0 is a separate DID parser in the case of MPEG-21.

Other modules are the same functions as explained in the above.

In Figure 6 it is shown for the Terminal Processing Flow Chart to process protection & Packaging Information carried in REL-IPMP Control Graph before a protected content could be consumed in module 6.18.

Module 6.1 is to parse DID and REL-IPMP Control Graph information where DID parser is required only for the case REL-IPMP Control Graph is carried in DID in MPEG-21 case.

In the case of content distribution over RTP network, REL-IPMP Control Graph can be retrieved from SDP to obtain rights and protection description information except the key information if it is time-variant.

Module 6.2 is to detect if the content is protected or free. If it is free, it will be able to play back by module 6.18 for consumption. Otherwise there are three branches to go and check in module 6.3, 6.4, and 6.5, respectively.

Module 6.3 is to detect if the Rights is encrypted, module 6.4 is to detect if the content is encrypted, and module 6.5 is to detect if the content is watermarked.

If the rights is protected, module 6.6 is to invoke the protection tool with ToolID and module 6.7 is to check the integrity of the rights using the tool. If the integrity is successfully verified in module 6.8, the rights will be sent to module 6.9 for parsing the rights by REL Engine which conforms to the existing REL standard.

Module 6.11 is to process the rights and conditions attached to the content and store the entitled rights and conditions in a buffer. In module 6.19 those rights requested by the users are subjected to checking against the rights and conditions stored in the buffer.

If there is license carried in Rights, module 6.10 is to retrieve license from License Manager which may be temper resistant (TR) protected.

If the content is protected and encrypted, module 6.13 is to invoke the encryption tool indicated by ToolID carried in REL-IPMP Control Graph, module 6.14 is to retrieve Key Information, and module 6.12 is to obtaining the key license from License Manager.

License Manager here could be protected by temper resistant technique if it is part of the terminal or somewhere in other places, since it will provide the actual license which the decryption engine will use to un-protect the content.

The encryption tool can be defined as default for most of the terminals to use in their implementation, while an IPMP ToolID is provided so that people can choose other than default encryption tool in their special domain or case. If the platform is allowed to download and use different encryption tool indicated by ToolID, it would achieve extensibility, flexibility and renewability at the same time we will achieve interoperability across different domains.

Key Information could be retrieved from different places in the case of content delivery via various networks. This will depend on where you place key information. If you place them in RTP header, you can get them there, while if you place them as other packets like video and audio data, you can get them by following the same rules applied to video and audio. The time-variant key information is required to obtain in the same time when you need to decrypt the video and audio content.

Module 6.15 is to decrypting the content with the invoked tool, KeyData, and License, then passed to module 6.17 for further processing.

If the content is detected as watermarked in module 6.5, the watermarking tool with ToolID and its description data including interface will be invoked and prepared in module 6.16 for action which is up to user's request.

Finally module 6.17 is to exercise the rights which user is requested based on the entitled rights & conditions, and act on the un-protected content which is the output of module 6.15.

In Figure 6 Temper Resistant is used to protect the functioning of License Manager to provide license, Rights & Condition Processing to prepare the rights, even content decryption for obtaining un-protected content.

Figure 9 shows for a modified IPMP Architecture with REL-IPMP Control Graph processed. Compared to the Rights and Protection (IPMP Related) functions in Figure 6 and Figure 9, it is clear that there are many IPMP related functions missing in the prior art of Figure 2. Only the blocks in blue color in Figure 6 which are the module 6.9 for REL Engine, module 6.10 and 6.12 for License Manager, and module 6.11 for Conditions Processing, are introduced in the prior art as shown in Figure 2. Such function blocks are module 2.1, module 2.4, and module 2.5 in Figure 2.

As shown in Figure 9, Module 9.11 is added for parsing and processing IPMP Control Graph information, and the corresponding results are passed to License Manager in module 9.4, REL related data passed to REL Engine in module 9.1 after its integrity is checked, and content protection and watermarking information passed to DI iNstanace in module 9.3 for further processing.

Decrypting, watermarking, etc. in module 9,12, could be conducted in module 9.8 if such method is defined in DIME, or in module 9.9 if it is defined as one function of DIBO, or in module 9.10 if it is an external function.

The line 9.14 is shown for the data flow from REL-IPMP Control Graph processing module to REL Engine, and the line 9.15 is shown for the data flow from REL-IPMP Control Graph processing module to NI iNstance.

The line 9.16 is shown for the data flow from License Manager to the un-protecting block in the module 9.12 for issuing a license.

Module 9.13 is for Event Reporting Engine which is placed in the same trusted domain compared to that in Figure 2.

TR means Temper Resistance module to be used to protect License Manager operation and Condition Processing Operation.

Other modules have the similar meaning as explained in Figure 2.

In Figure 10, Layout of Rights and Protection in IPMP Control Graph or REL-IPMP Control Graph is shown, where the content ID, the protected object's indicator, the protection flags, and the detail rights and conditions as well as the detail protection descriptions are placed and carried in this holder.

### 3.7 Effective of Invention

The invention is very effective when content is required to be protected with rights and conditions, especially such content can be in any data form and could be transmitted via various network.

The invention is effective when such protection is required to associate with the protected content via content ID, especially such protection information is defined as a set of descriptions attached to the protected content using content ID, or DII in MPEG-21;

The invention is effective when such protection is placed in a generic IPMP Control Graph holder or REL-IPMP Control Graph holder, which is clean and convenient for content creation, content distribution, as well as content consumption, and such holder could be carried in DID in MPEG-21 static file format or carried in SDP for RTP transmission.

The invention is effective when each of the protection is indicated by ToolID so that both defined IPMP tool and external IPMP Tool can be used for flexibility, renewalbility and extensibility;

## 4 BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a Prior Art: DID Structure with Possible Protection Information Included

Figure 2 shows a Prior Art: MPEG-21 IPMP Architecture

Figure 3 shows Content Packaging Flow Chart with separate Rights & Protection

Figure 4 shows Terminal Processing Flow Chart for Protected & Packaged Content with IPMP Control Graph Information

Figure 5 shows Content Packaging Flow Chart with mixed Rights & Protection

Figure 6 shows Terminal Processing Flow Chart for Protected & Packaged Content with REL-IPMP Control Graph Information

Figure 7 shows IPMP Control Graph for Rights & Protection Information Carried in DID

Figure 8 shows IPMP Architecture with IPMP Control Graph Processed

Figure 9 shows IPMP Architecture with REL-IPMP Control Graph Processed

Figure 10 shows Layout of Rights and Protection in REL-IPMP Control Graph

## 6 REFERENCE

[1] "ISO/IEC 21000-2 MPEG-21 Digital Item Declaration FDIS", *ISO/IEC JTC1 SC29/WG11/N4813, May 2002*
[2] Patent on "Apparatus of a MPEG-21 System", inventors: **Zhongyang Huang, Ming Ji, Shengmei Shen, Taka Senoh, Takuyo Kogure, Takafumi Ueno** with internal patent number Pat01.028, filed in Japan in Feb.2002.
[3] "MPEG-21 Architecture, Scenarios and IPMP Requirements", *ISO/IEC JTC1 SC29/WG11/N5874*, July 2003

【書類名】外国語図面

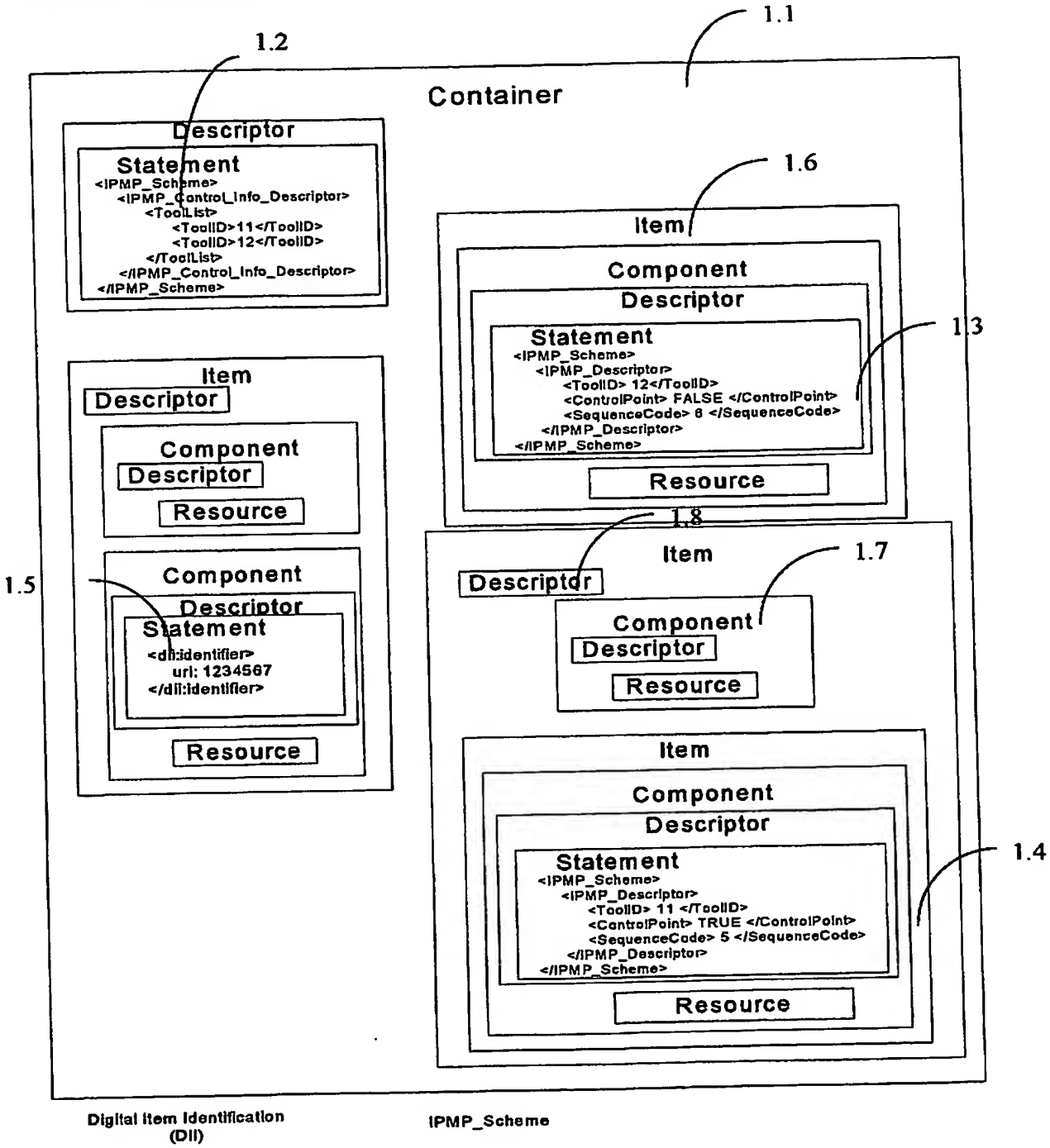


Figure 1

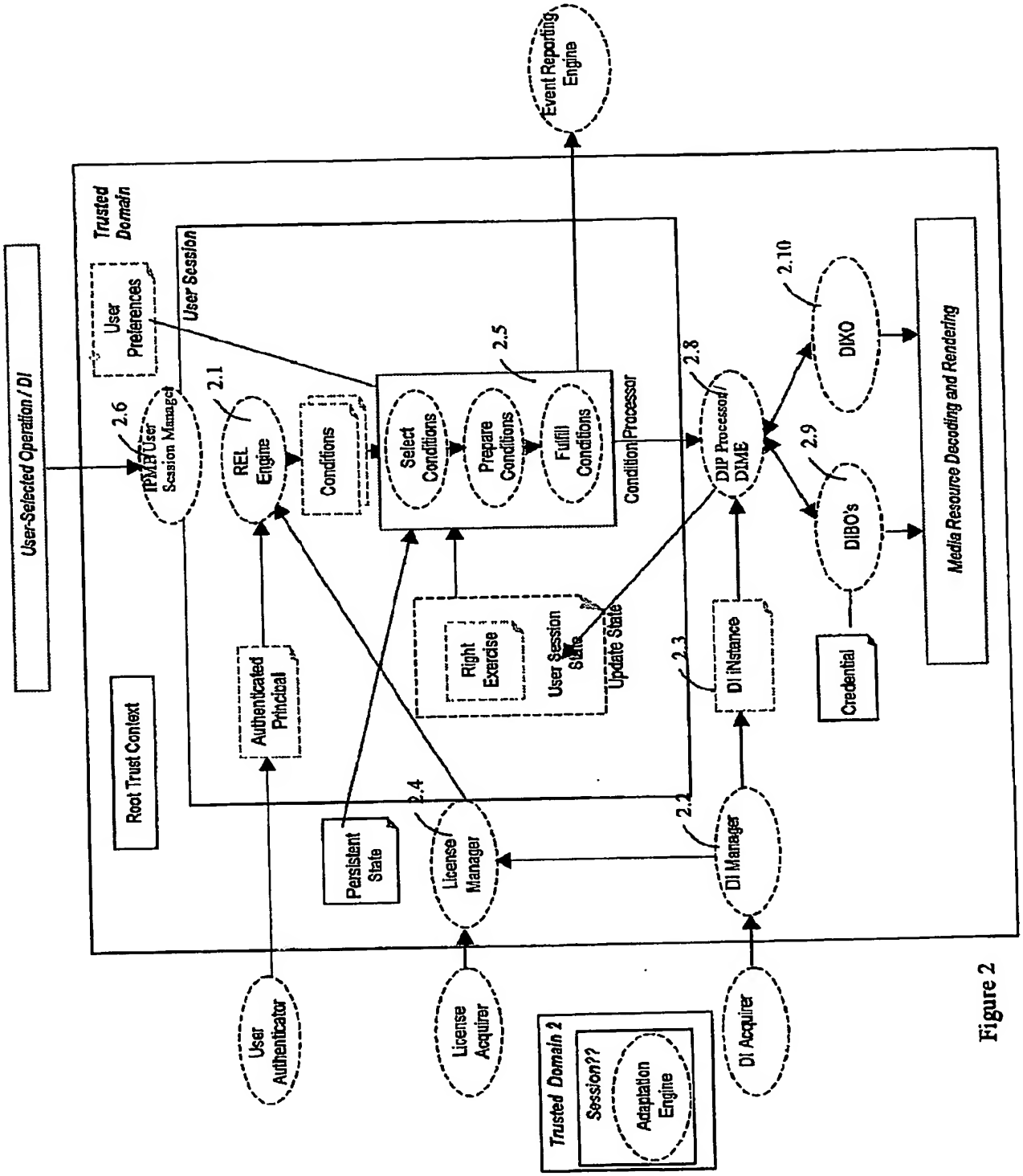
Event Reporting Engine
Trusted Domain
User Session
User Preferences
User-Selected Operation / DI
IPMP/User Session Manager
2.6
2.1
REL Engine
Conditions
Select Conditions
Prepare Conditions
Fulfill Conditions
Condition Processor
2.5
2.8
DIP Processor/ DIME
2.10
DIKO
2.9
DIBO's
Media Resource Decoding and Rendering
Root Trust Context
Authenticated Principal
Right Exercise
User Session State
Update State
2.3
DI Instance
Credential
Persistent State
2.4
License Manager
2.2
DI Manager
User Authenticator
License Acquirer
Trusted Domain 2
Session??
Adaptation Engine
DI Acquirer

Figure 2

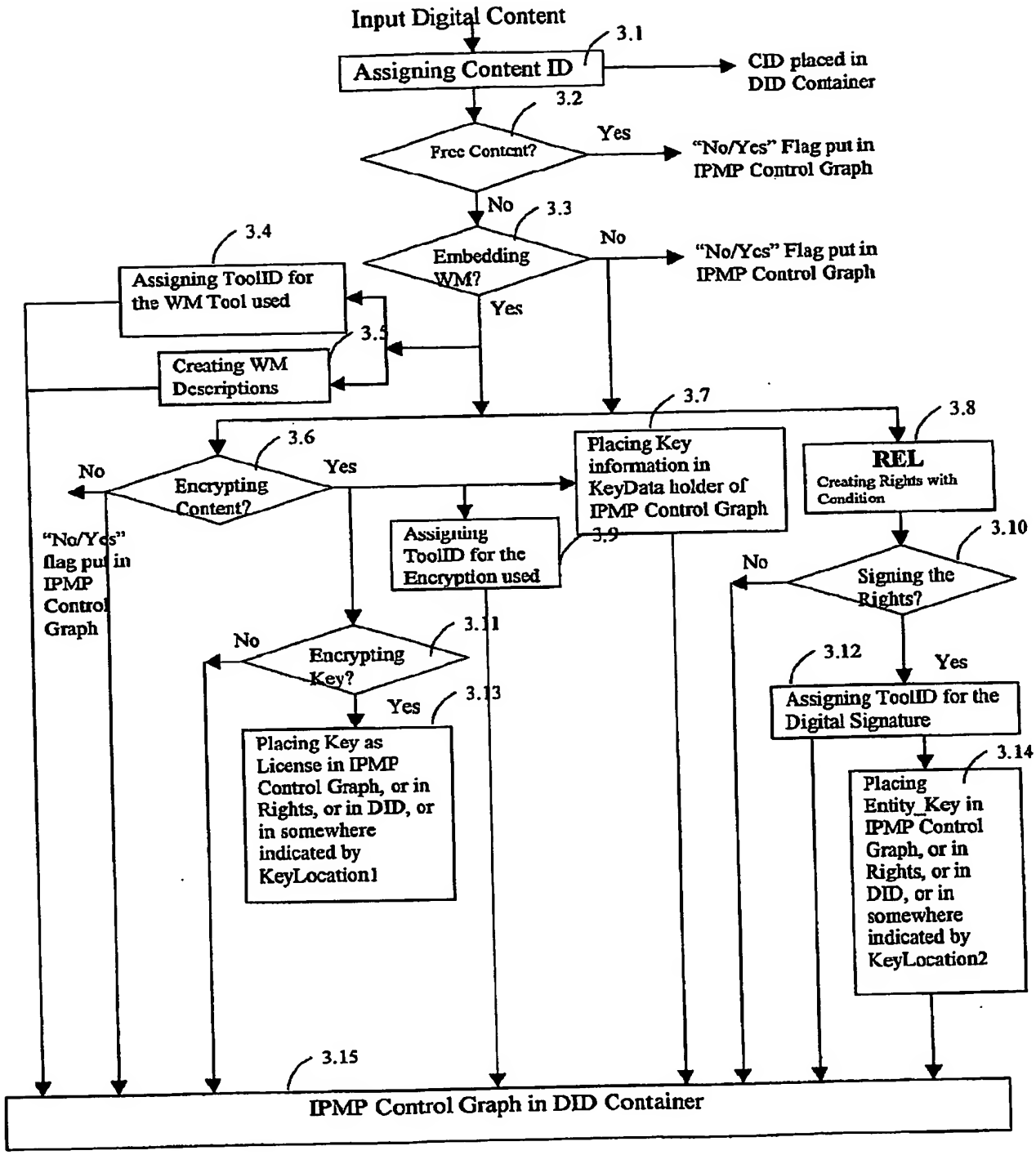
Input Digital Content
Assigning Content ID
3.1
CID placed in DID Container
Free Content?
3.2
Yes
"No/Yes" Flag put in IPMP Control Graph
No
Embedding WM?
3.3
No
"No/Yes" Flag put in IPMP Control Graph
Yes
Assigning ToolID for the WM Tool used
3.4
Creating WM Descriptions
3.5
3.7
3.8
Encrypting Content?
3.6
No
Yes
Placing Key information in KeyData holder of IPMP Control Graph
REL
Creating Rights with Condition
"No/Yes" flag put in IPMP Control Graph
Assigning ToolID for the Encryption used
3.9
3.10
No
Signing the Rights?
Encrypting Key?
3.11
No
Yes
3.12
Assigning ToolID for the Digital Signature
3.13
Yes
Placing Key as License in IPMP Control Graph, or in Rights, or in DID, or in somewhere indicated by KeyLocation1
3.14
Placing Entity_Key in IPMP Control Graph, or in Rights, or in DID, or in somewhere indicated by KeyLocation2
3.15
IPMP Control Graph in DID Container

Figure 3

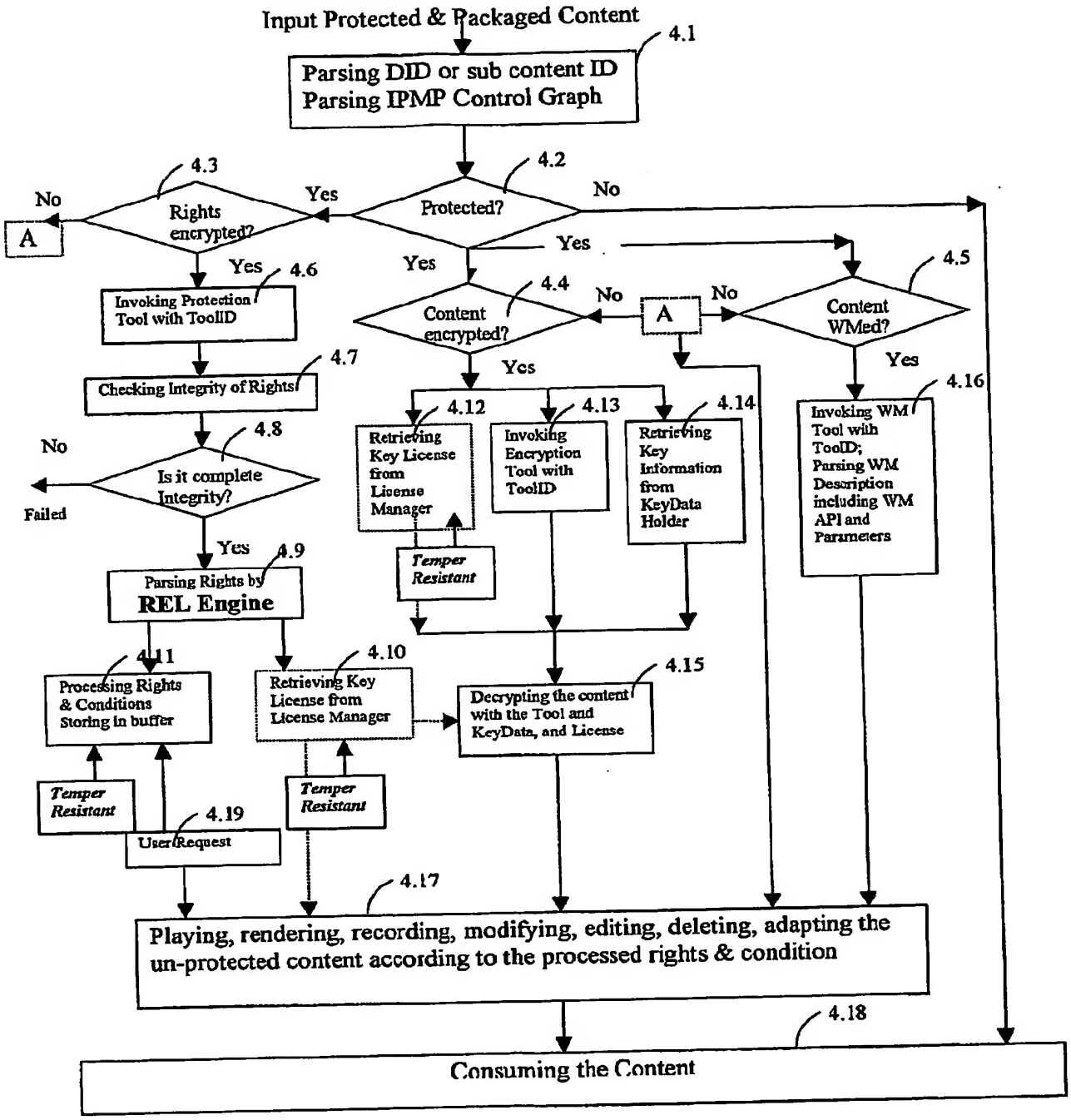
Input Protected & Packaged Content
4.1
Parsing DID or sub content ID
Parsing IPMP Control Graph
4.2
Protected?
No
Yes
4.3
Rights encrypted?
No
A
Yes
4.6
Invoking Protection Tool with ToolID
4.7
Checking Integrity of Rights
4.8
Is it complete Integrity?
No
Failed
Yes
4.9
Parsing Rights by REL Engine
4.11
Processing Rights & Conditions Storing in buffer
4.10
Retrieving Key License from License Manager
Temper Resistant
Temper Resistant
4.19
User Request
Yes
4.4
Content encrypted?
No
A
No
4.5
Content WMed?
Yes
Yes
4.12
Retrieving Key License from License Manager
4.13
Invoking Encryption Tool with ToolID
4.14
Retrieving Key Information from KeyData Holder
Temper Resistant
4.15
Decrypting the content with the Tool and KeyData, and License
4.16
Invoking WM Tool with ToolID; Parsing WM Description including WM API and Parameters
4.17
Playing, rendering, recording, modifying, editing, deleting, adapting the un-protected content according to the processed rights & condition
4.18
Consuming the Content

Figure 4

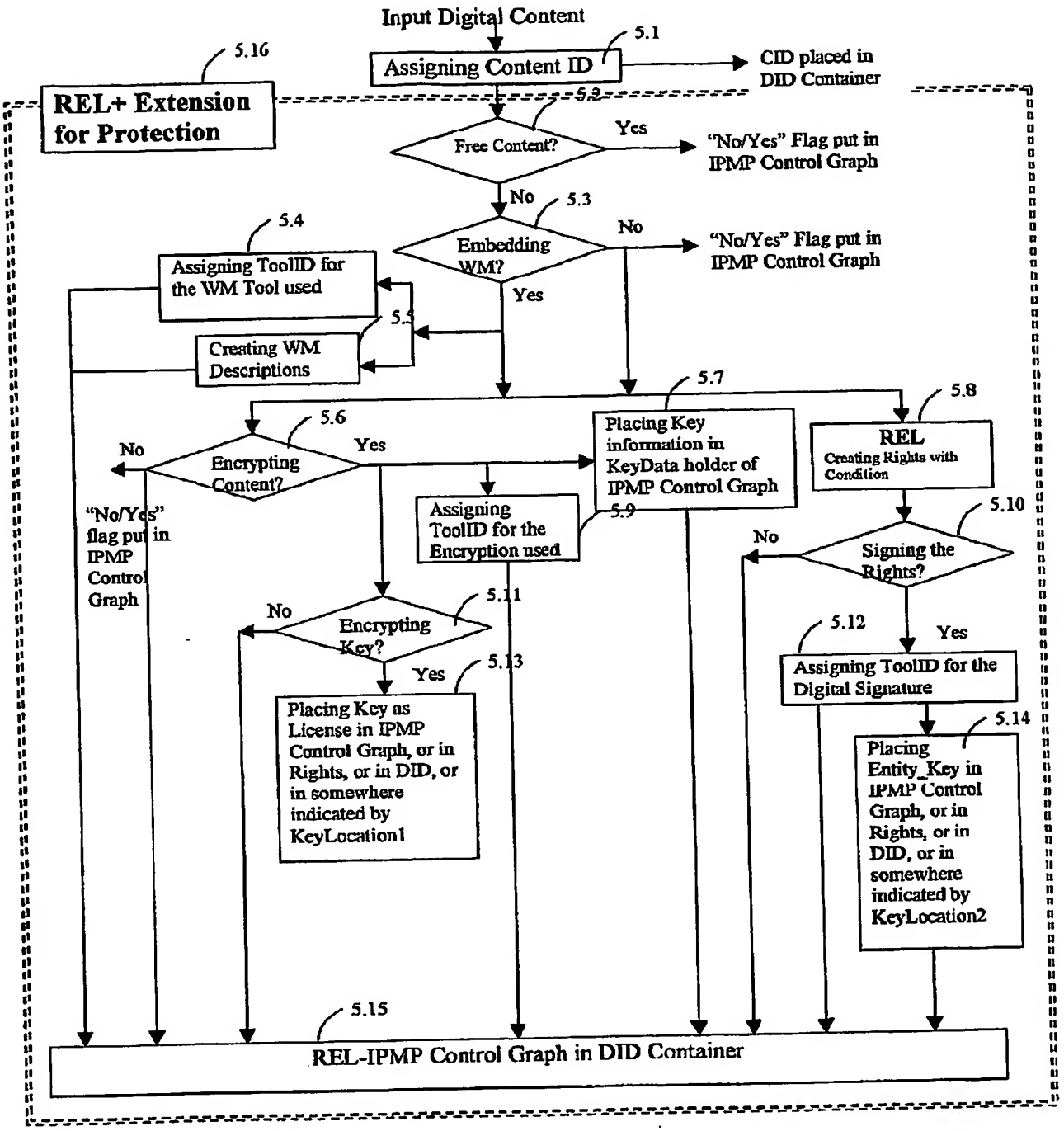
Input Digital Content
5.1
Assigning Content ID
CID placed in DID Container
5.16
REL+ Extension for Protection
5.2
Free Content?
Yes
"No/Yes" Flag put in IPMP Control Graph
No
5.3
Embedding WM?
No
"No/Yes" Flag put in IPMP Control Graph
Yes
5.4
Assigning ToolID for the WM Tool used
5.5
Creating WM Descriptions
5.7
5.8
5.6
No
Encrypting Content?
Yes
Placing Key information in KeyData holder of IPMP Control Graph
REL
Creating Rights with Condition
"No/Yes" flag put in IPMP Control Graph
Assigning ToolID for the Encryption used
5.9
5.10
No
Signing the Rights?
5.11
No
Encrypting Key?
5.12
Yes
Assigning ToolID for the Digital Signature
Yes
5.13
Placing Key as License in IPMP Control Graph, or in Rights, or in DID, or in somewhere indicated by KeyLocation1
5.14
Placing Entity_Key in IPMP Control Graph, or in Rights, or in DID, or in somewhere indicated by KeyLocation2
5.15
REL-IPMP Control Graph in DID Container

Figure 5

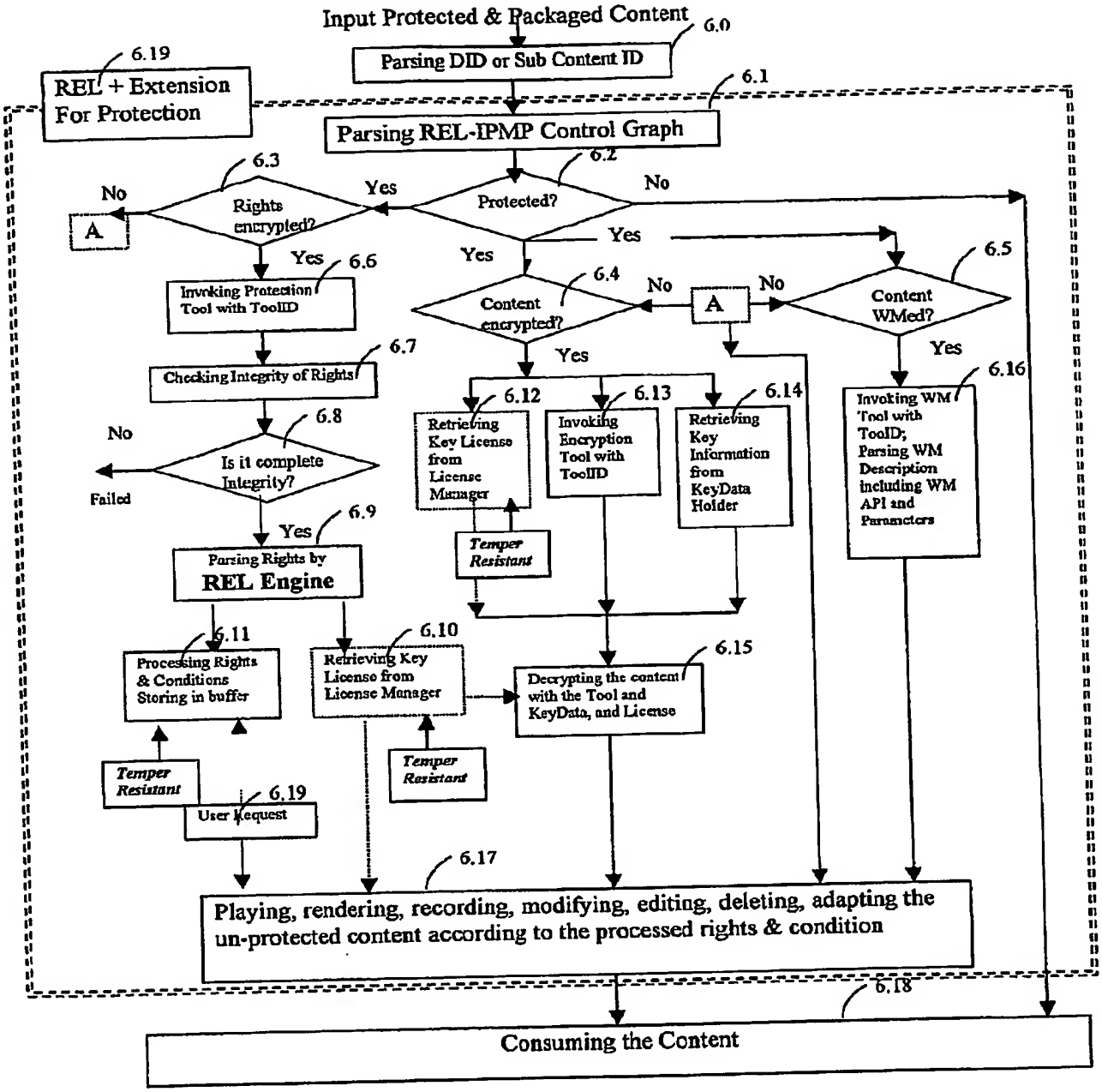
Input Protected & Packaged Content
6.0
Parsing DID or Sub Content ID
6.19
REL + Extension For Protection
6.1
Parsing REL-IPMP Control Graph
6.3
Rights encrypted?
No
Yes
A
6.2
Protected?
No
Yes
Yes
6.5
Content WMed?
No
A
6.4
Content encrypted?
No
Yes
Yes
6.6
Invoking Protection Tool with ToolID
6.7
Checking Integrity of Rights
6.8
Is it complete Integrity?
No
Failed
Yes
6.9
Parsing Rights by REL Engine
6.12
Retrieving Key License from License Manager
6.13
Invoking Encryption Tool with ToolID
6.14
Retrieving Key Information from KeyData Holder
6.16
Invoking WM Tool with ToolID; Parsing WM Description including WM API and Parameters
Temper Resistant
6.11
Processing Rights & Conditions Storing in buffer
6.10
Retrieving Key License from License Manager
6.15
Decrypting the content with the Tool and KeyData, and License
Temper Resistant
Temper Resistant
6.19
User Request
6.17
Playing, rendering, recording, modifying, editing, deleting, adapting the un-protected content according to the processed rights & condition
6.18
Consuming the Content

Figure 6

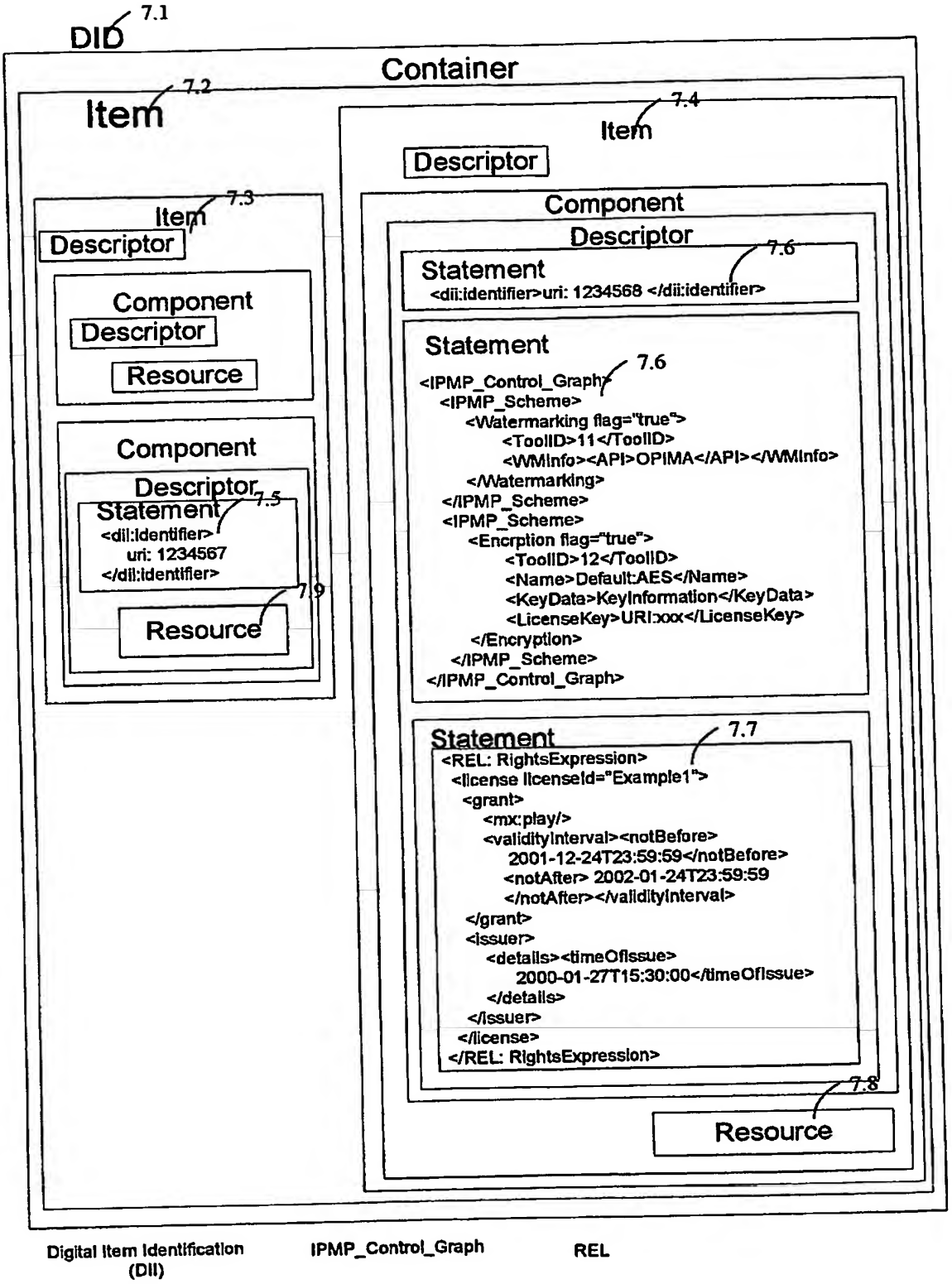
DID
7.1
Container
Item
7.2
Item
7.4
Descriptor
Item
7.3
Descriptor
Component
Descriptor
Resource
Component
Descriptor
Statement
7.5
<dii:identifier>
uri: 1234567
</dii:identifier>
Resource
7.9
Component
Descriptor
Statement
7.6
<dii:identifier>uri: 1234568 </dii:identifier>
Statement
7.6
<IPMP_Control_Graph>
<IPMP_Scheme>
<Watermarking flag="true">
<ToolID>11</ToolID>
<WMInfo><API>OPIMA</API></WMInfo>
</Watermarking>
</IPMP_Scheme>
<IPMP_Scheme>
<Encrption flag="true">
<ToolID>12</ToolID>
<Name>Default:AES</Name>
<KeyData>KeyInformation</KeyData>
<LicenseKey>URI:xxx</LicenseKey>
</Encryption>
</IPMP_Scheme>
</IPMP_Control_Graph>
Statement
7.7
<REL: RightsExpression>
<license licenseId="Example1">
<grant>
<mx:play/>
<validityInterval><notBefore>
2001-12-24T23:59:59</notBefore>
<notAfter> 2002-01-24T23:59:59
</notAfter></validityInterval>
</grant>
<issuer>
<details><timeOfIssue>
2000-01-27T15:30:00</timeOfIssue>
</details>
</issuer>
</license>
</REL: RightsExpression>
7.8
Resource
Digital Item Identification (DII)
IPMP_Control_Graph
REL

**Figure 7 (a)**

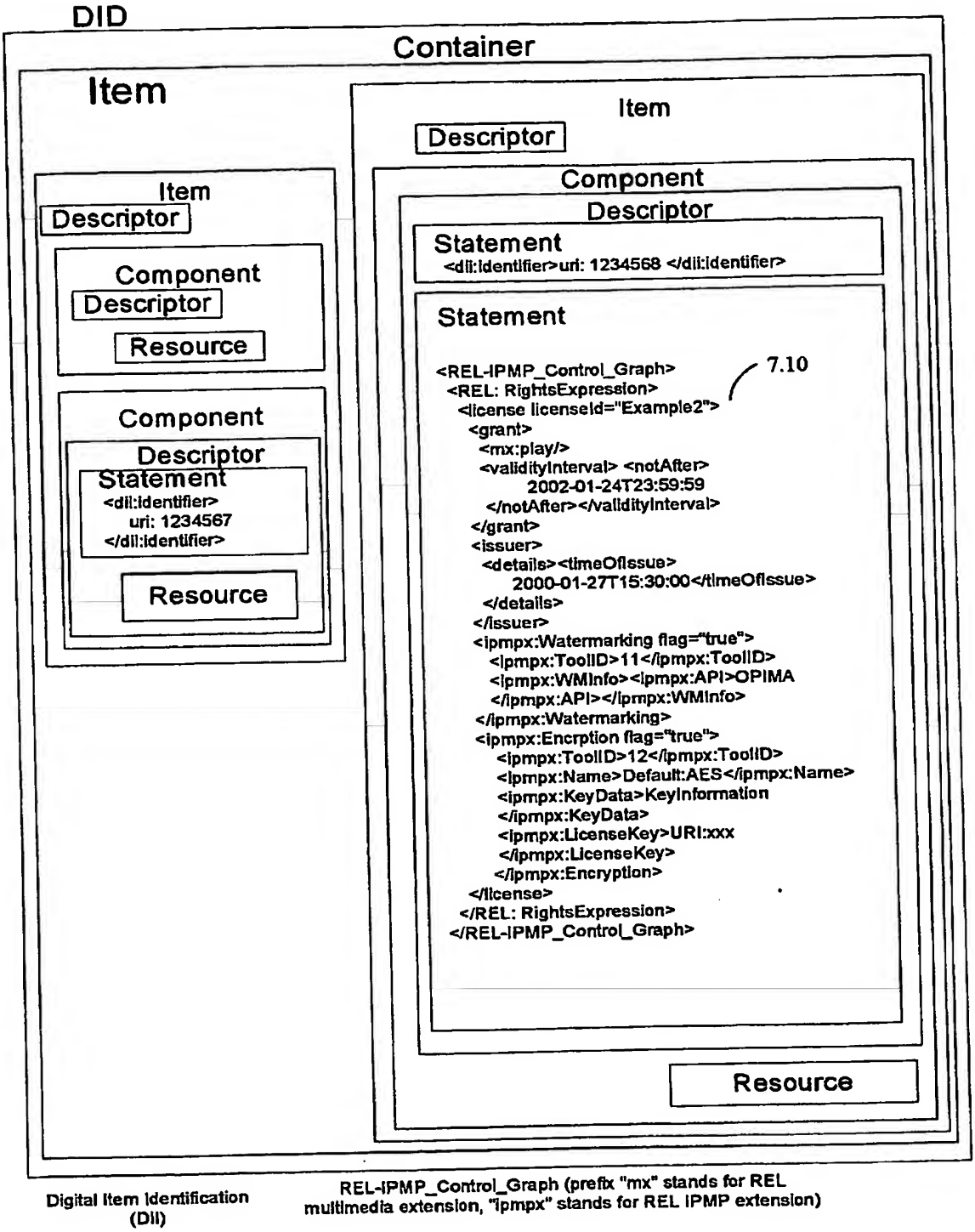
DID
Container
Item
Item
Descriptor
Item
Descriptor
Component
Descriptor
Resource
Component
Descriptor
Statement
<dii:identifier>
uri: 1234567
</dii:identifier>
Resource
Component
Descriptor
Statement
<dii:identifier>uri: 1234568 </dii:identifier>
Statement
<REL-IPMP_Control_Graph>
<REL: RightsExpression>
<license licenseId="Example2">
<grant>
<mx:play/>
<validityInterval> <notAfter>
2002-01-24T23:59:59
</notAfter></validityInterval>
</grant>
<issuer>
<details><timeOfIssue>
2000-01-27T15:30:00</timeOfIssue>
</details>
</issuer>
<ipmpx:Watermarking flag="true">
<ipmpx:ToolID>11</ipmpx:ToolID>
<ipmpx:WMInfo><ipmpx:API>OPIMA
</ipmpx:API></ipmpx:WMInfo>
</ipmpx:Watermarking>
<ipmpx:Encrption flag="true">
<ipmpx:ToolID>12</ipmpx:ToolID>
<ipmpx:Name>Default:AES</ipmpx:Name>
<ipmpx:KeyData>KeyInformation
</ipmpx:KeyData>
<ipmpx:LicenseKey>URI:xxx
</ipmpx:LicenseKey>
</ipmpx:Encryption>
</license>
</REL: RightsExpression>
</REL-IPMP_Control_Graph>
7.10
Resource
Digital Item Identification (DII)
REL-IPMP_Control_Graph (prefix "mx" stands for REL multimedia extension, "ipmpx" stands for REL IPMP extension)

**Figure 7 (b)**

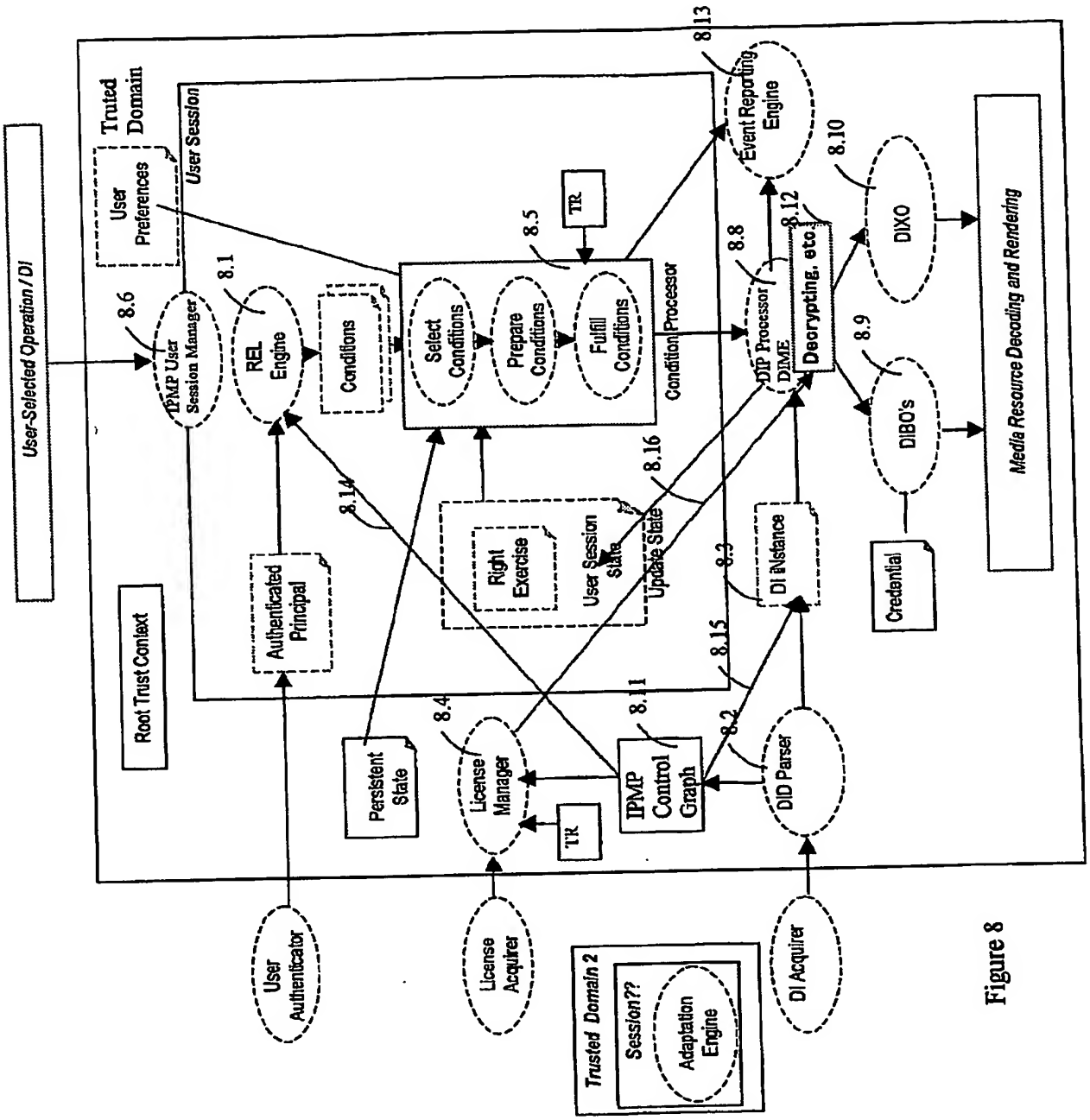
User-Selected Operation / DI
Truted Domain
User Preferences
User Session
IPMP User Session Manager
REL Engine
Conditions
Select Conditions
Prepare Conditions
Fulfill Conditions
Condition Processor
TR
Event Reporting Engine
DIP Processor
DIME
Decrypting, etc.
DIXO
DIBO's
Credential
Media Resource Decoding and Rendering
Authenticated Principal
Right Exercise
User Session State
Update State
DI Instance
Root Trust Context
Persistent State
License Manager
IPMP Control Graph
DID Parser
User Authenticator
License Acquirer
DI Acquirer
Trusted Domain 2
Session??
Adaptation Engine
8.1
8.2
8.3
8.4
8.5
8.6
8.8
8.9
8.10
8.11
8.12
8.13
8.14
8.15
8.16

Figure 8

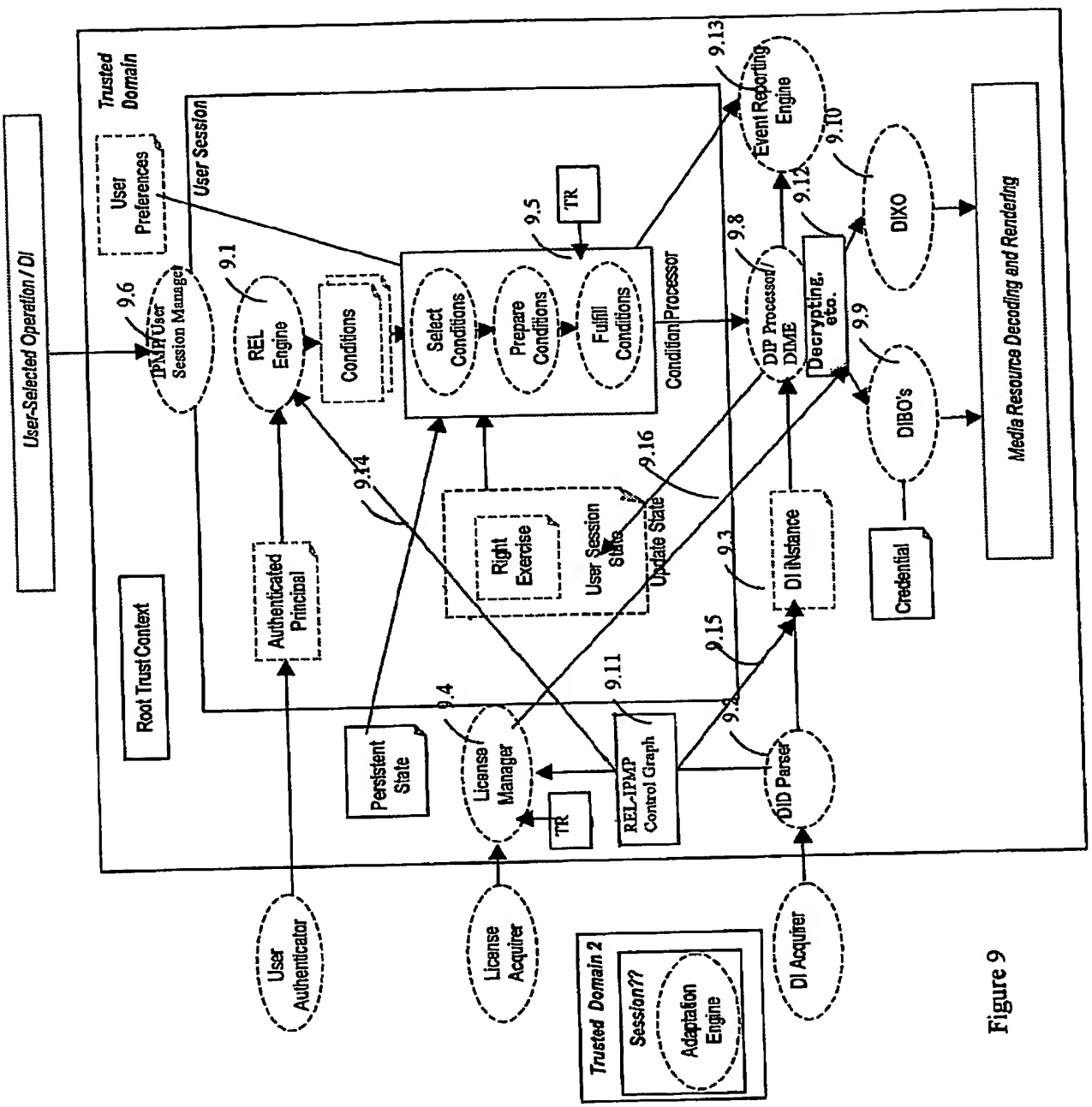
User-Selected Operation / DI
Trusted Domain
User Preferences
User Session
IPMP User Session Manager
9.6
9.1
REL Engine
Conditions
Select Conditions
Prepare Conditions
Fulfill Conditions
Condition Processor
9.5
TR
9.13
Event Reporting Engine
9.10
9.12
9.8
DIP Processor / DIME
Decrypting, etc.
DIXO
DIBO's
9.9
Media Resource Decoding and Rendering
Root Trust Context
Authenticated Principal
9.14
Right Exercise
User Session State
Update State
9.16
DI Instance
9.3
Credential
9.15
Persistent State
License Manager
9.4
TR
REL-IPMP Control Graph
9.11
9.7
DID Parser
User Authenticator
License Acquirer
Trusted Domain 2
Session??
Adaptation Engine
DI Acquirer

Figure 9

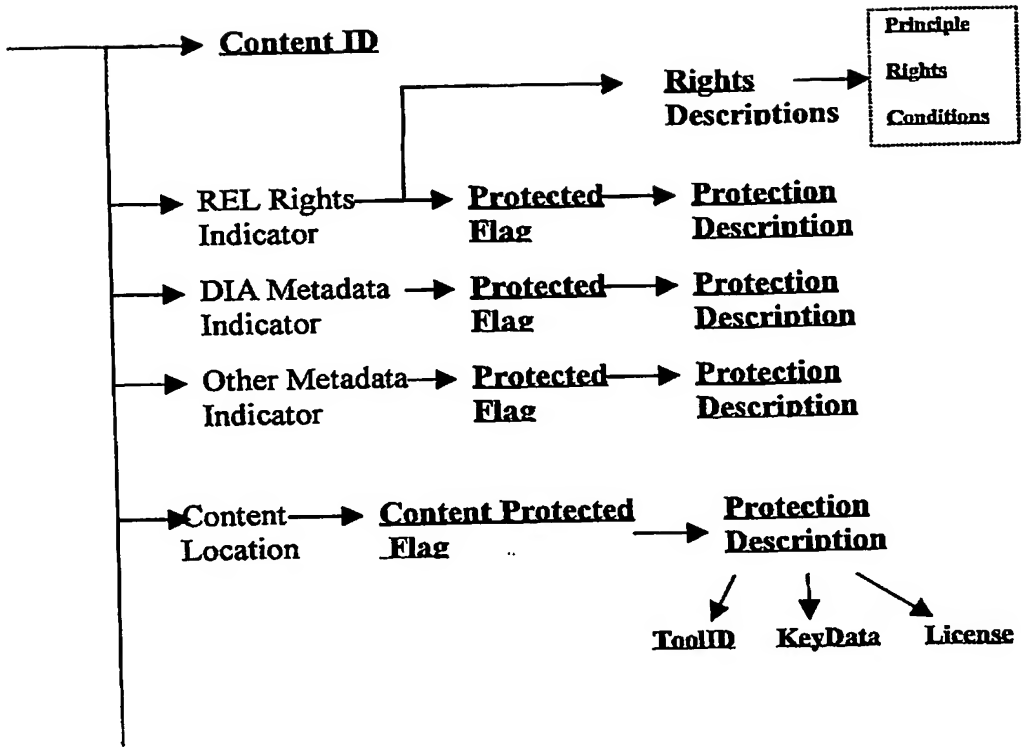
Content ID
Rights Descriptions
Principle
Rights
Conditions
REL Rights Indicator
Protected Flag
Protection Description
DIA Metadata Indicator
Protected Flag
Protection Description
Other Metadata Indicator
Protected Flag
Protection Description
Content Location
Content Protected Flag
Protection Description
ToolID
KeyData
License

Figure 10

【書類名】外国語要約書

## 5 ABSTRACT

The invention is related to Digital Rights Management (DRM) or Intellectual Property Management and Protection (IPMP) for a generic digital content. The concept of IPMP Control Graph and REL-IPMP Control Graph is introduced to carry protection signalling and rights expression data. Both content packaging and terminal processing relating to the above control graph are clearly defined and elaborated.

特願２００３－３５３６９１

# 出願人履歴情報

識別番号　[０００００５８２１]

１．変更年月日　１９９０年　８月２８日
[変更理由]　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社